Privacy Impact Assessment

1. DoD Component: Defense Logistics Agency.

2. Name of IT System: N/A.

3. Identification Number: N/A.

4. IT Investment (OMB Circular A-11) Unique Identifier: N/A.

5. Privacy Act System of Records Notice Identifier: S500.50, Facility Access Records.

6. OMB Information Collection Requirement Number and Expiration Date: N/A.

7. Authority: 5 U.S.C. Chapter 3, Powers; 5 U.S.C. 6122, Flexible Schedules, agencies authorized to use; 10 U.S.C. 133, Under Secretary of Defense for Acquisition and Technology; U.S.C. 403 et seq., Highway Safety Research and Development; E.O. 9397 (SSN); and E.O. 10450 (Security Requirements for Government Employees) as amended.

8. Brief summary/Overview of the IT system:

This is a database of individuals requiring access to Defense Logistics Agency controlled facilities, buildings, and parking lots. It is used primarily to record the issue of short- and long-term facility access badges and vehicle decals. It is also used to issue child identification cards, when requested by parents, in support of agency morale programs. Because the collection of data on children of the workforce triggers the requirement for a Privacy Impact Assessment, this document will only address that aspect of the database.

Child data is manually keyed into the system from input records provided by the parent. The child's photograph is taken and added to the child's file. The system generates a plastic badge containing the child's photograph, name, and descriptive data. Where a parent requests an updated or replacement badge, the original data is retrieved by child's name, SSN, or child badge number (if known by the parent), and the updated information is keyed into the system.

9. Identifiable information to be Collected and Nature and Source: The database relies on these personal identifiers: Child's name, child's Social Security Number, or child identification badge number. All information is supplied by the child's parent except the badge number and the current photograph which are provided by the Security Operations Division.

10. Purpose of the Collection: The purpose of the program is to capture critical descriptive data about a child, along with a current photograph, for parental use should a child go missing. Data is collected in support of Department of Defense morale, welfare, and recreation programs.

11. Data Uses: Data is used to create and issue a child identification badge. The child's data resides on the system to facilitate replacing lost badges or issuing updated ones. The data is not used for any other internal purposes.

12. Internal and External Data Sharing: The segment of the database involving children of the workforce will be shared as follows:

Internal: Data may be viewed by or shared with employees, military members, and contractors assigned to the DLA Public Safety directorate for purposes of issuing new and replacement child identification badges. The data may also be accessed by individuals, including contractors, assigned to provide software/database technical support.

External: Information collected for child identification badges is not shared with external entities, except to the extent that the parent might be regarded as "external."

13. Opportunities to object to the collection or to consent to the specific uses and how consent is granted:

A Privacy Act system notice will be published in the Federal Register with a 30 day public comment period. Forms that collect personal data will contain a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data or participating in the program. The Statement advises that participation is voluntary. The only consequence for those who choose not to participate is that DLA will be unable to issue a child badge. Individuals may raise an objection with the HQ DLA Privacy Act office during the comment period, during data collection, or at any time after the program is launched. If no objections are received, consent is presumed.

14. Information provided the individual at collection, the format, and the means of delivery:

– Privacy Act Statements, as required by 5 U.S.C. 552a(e)(3), are provided at the collection point. The Statement provides the following: collection purpose, authorities, external uses, the voluntary nature of the program, the fact that no consequences accrue for those who choose not to participate, the name and number of the Privacy Act system notice governing the collection, and an electronic link to the system notice. The Statement is included on paper and electronic collection forms.

– DLA Fair Information Principles, which govern all Privacy Act data collections, are published on the HQ DLA Home page. While not provided at the collection point, the Principles are contained in DLA Privacy Act training module "Privacy Act 101" – mandatory training for all DLA employees, military members, and contractors. The DLA workforce is required to be aware of the Principles to fulfill their duties in handling third party personal data and in learning their Privacy Act rights.

15. Data Controls:

Administrative: Users, including individuals responsible for system maintenance, receive initial and periodic refresher Privacy Act and Information Assurance training. User are warned through log-on procedures of the conditions associated with access and the consequences of improper activities. Users are required to accept those conditions/consequences before logon completes. Users are trained to lock their workstations when leaving them unattended, to shut down computers when leaving at the end of the duty shift, and to be alert to third parties entering the workspace. Data is periodically backed up and stored on a separate server.

Physical: The data resides on a stand-alone computer system that is not connected to the World Wide Web. Central Processing Units are located in a physically controlled buildings with either a badge/card swipe or read required for entry. Within buildings, central processing units are kept in locked or controlled access areas. Data entry terminals are located in individual rooms or security bunkers with lockable doors or controlled access protocols. Where possible,

office layout is designed to keep computer terminals protected from the view of room/bunker visitors. All terminals are equipped with filtering devices that blacken the screen from angular views. Electronic records are backed up periodically. Areas housing central processing units, servers, and work stations are configured with a water-based fire suppression system. Should the system fail, the lost data could be constructed from the back-up records, paper files, and input sources.

Technical: Data is initially uploaded to the stand-alone via compact disk (CD). The CD is created from data initially gathered on a system fully certified and accredited under DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process. That system uses built-in virus detection software with a notification system in place to alert all users to new viruses and software-resistant viruses. Computer terminals are password controlled with system-generated forced password change protocols. All passwords are tested for strength at the time of selection. Computer screens automatically lock after a preset period of inactivity with re-entry controlled by passwording. Systems manually locked by the user also require passwording for reentry. Shutdown compliance is periodically checked. Workstations connecting to the system have real time virus/worm detection software installed.

16. Privacy Act Interface: This system is covered by an existing Privacy Act Systems of Records notice, S500.50, Facility Access Records.

17. Potential threats in collecting, using, and sharing the information; dangers in providing notices or opportunities to object/consent or to providing notices to the individual; risks posed by the adopted security measures:

Threats: Data is collected and used in a dedicated security mode. Data sharing occurs only among individuals authorized access to the system as stated in the governing Privacy Act system notice. Data screens are marked with the "For Official Use Only" data handling legend. All system users are made aware of restrictions on secondary uses of the data by initial and refresher Privacy Act and Information Assurance training.

Dangers: There are no dangers in providing notice of the collection or allowing an individual to object/consent. Therefore, individuals are given this opportunity at times of notice publication and data collection. Afterwards, individuals may raise objections if new threats are perceived.

Risks: The security risks associated with maintaining data in an electronic environment have been mitigated through administrative, technical, and physical safeguards described in this document. The safeguards in place are commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the data.

18. Other analysis prepared; status of the system as a "major information system." A Risk Assessment was also prepared for this system. This database does not constitute a major information system for OMB Circular A-130 purposes.

19. Publication of Privacy Impact Assessment: This document will be published either in full or in summary form on the DLA public website, http://www.dla.mil/public_info/efoia/privacy.asp.

Preparing Official: [redacted] 6 Sep 05
(Signature) (Date)

Name: FRANK NEKOBA
Title: Staff Director, Public Safety, DLA Enterprise Support
Phone:

Security Officer: [redacted] 8 Sep 05
(Signature) (Date)

Name: [redacted]
Title: Information Assurance Manager
Phone:

Privacy Officer: [redacted] 25 Aug 05
(Signature) (Date)

Name: SUSAN SALUS
Title: HQ DLA Privacy Act Officer
Phone:

Reviewing Official: [redacted] SEP 22 2005
(Signature) (Date)

Name: MAE DE VINCENTIS
Title: DLA Chief Information Officer
Phone: